Second Edition

AWS® Certified Security STUDY GUIDE

SPECIALTY (SCS-C02) EXAM

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

2 custom practice exams

Over 100 electronic flashcards

Searchable key term glossary

MAURICIO MUÑOZ, DARÍO GOLDFARB,
ALEXANDRE M.S.P. MORAES, OMNER BARAJAS,
ANDRÉS GONZÁLEZ SANTOS, ROGERIO KASA

SYBEX®
A Wiley Brand

AWS®

Certified Security Study Guide

Specialty (SCS-C02) Exam

Second Edition

AWS®

Certified Security Study Guide

Specialty (SCS-C02) Exam

Second Edition

Mauricio Muñoz, Darío Goldfarb,
Alexandre Matos da Silva Pires de Moraes, Omner Barajas,
Andrés González Santos, Rogerio Kasa

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

The manufacturer' s authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: `Product_Safety@wiley.com`.

Library of Congress Control Number: 2025911987

ISBN: 9781394253463 (paperback)
ISBN: 9781394253470 (epub)
ISBN: 9781394253487 (ePDF)

Cover Design: Wiley
Cover Image: © Jeremy Woodhouse/Getty Images

Acknowledgments

First and foremost, we offer our most profound thanks to our spouses, children, and families, whose support and understanding during our many long hours of writing and reviews gave us the time and strength to create this book. This book would not have been possible without our wonderful families.

We would also like to show our appreciation for Amazon Web Services (AWS) for providing cloud-computing platforms, APIs, and the Specialty Exam to the world at large. We are excited to be an active part of this transformative growth and development of secure cloud computing in the world today.

We'd also like to thank associate publisher Jim Minatel and acquisitions editor Ken Brown for entrusting us with the role of creating this study guide for Wiley. We also appreciate the insights of technical editor Rogerio Kasa, whose attention to detail elevated this book to the next level. Thanks also goes to managing editor Pete Gaughan, project manager Robyn Alvarez, production specialist Bala Shanmugasundaram, copy editor Kezia Endsley, and the entire team at Wiley for their guidance and assistance in making this book. We'd also like to thank all of our colleagues and experts who consulted with us while we were writing this book—too many to name here, but we are grateful for your suggestions and contributions.

And perhaps more than anyone else, we would like to thank our readers. We are grateful for the trust that you have placed in us to help you study for the exam. We wrote this book to support you in your journey.

—The Authors

About the Authors

Mauricio Muñoz is a Principal Technologist at Amazon Web Services (AWS), where he guides global customers in their journey to implement mission-critical applications into the AWS Cloud. With over 25 years of experience in information security and a CISSP certification since 2005, Mauricio has continuously expanded his expertise across various domains, including networking, application integration, analytics, and cloud computing. A passionate advocate for learning and knowledge sharing, Mauricio has served as an authorized instructor for CISSP and CEH certification training, as well as other technical certifications, including recent AWS architectural training. He is a sought-after speaker at both cloud computing and industry events, bringing valuable insights to diverse audiences. His international career spans Latin America and the United States, enriching his global perspective in technology consulting. Academically, Mauricio holds an electronics engineering degree from Pontificia Universidad Javeriana (PUJ—Colombia) and an executive MBA from Insper (Brazil), combining technical prowess with strategic business acumen.

Darío Goldfarb is a security solutions architect at Amazon Web Services in Latin America with more than 18 years of experience in cybersecurity, helping organizations from different industries improve their cyber-resiliency. Dario enjoys sharing security knowledge through speaking at public events, presenting webinars, teaching classes for universities, and writing blogs and articles for the press. He has a significant number of certifications, including CISSP, the Open Group Master IT Architect, and the AWS Security Specialty certification, and he holds a degree in systems engineering from UTN (Argentina) and a diploma in cybersecurity management from UCEMA (Argentina).

Alexandre Matos da Silva Pires de Moraes, CCIE No. 6063, worked as a systems engineer for Cisco Brazil from 1998 to 2014, in projects involving not only security and VPN technologies but also routing protocol and campus design, IP multicast routing, and MPLS networks design. He is the author of *Cisco Firewalls* (Cisco Press, 2011) and has delivered many technical sessions related to security in market events, such as Cisco Networkers and Cisco Live (Brazil, United States, United Kingdom). In 2014, Alexandre started a new journey as a director for Teltec Solutions, a Brazilian systems integrator that is highly specialized in the fields of network design, security architectures, and cloud computing. Alexandre holds the CISSP and three CCIE certifications (routing/switching, security, and service provider). He graduated with a degree in electronic engineering from the Instituto Tecnológico de Aeronáutica (ITA—Brazil) and holds a master's degree in mathematics (group theory) from Universidade de Brasília (UnB—Brazil). Alexandre also contributes, as a mathematics teacher, to preparing candidates for the national exams of military universities in Brazil, such as ITA and IME (Instituto Militar de Engenharia).

Andrés González Santos is a senior security specialist solution architect at Amazon Web Services in Latin America with more than 20 years of experience in cybersecurity. Andrés has served in various security positions, including consultant, IT architect, and security

auditor, helping organizations across diverse industries strengthen their security posture. His experience spans multiple countries, including Colombia, Ecuador, and Peru, where he has implemented strategic technological solutions for both national and international enterprises. Andrés holds a master's degree in systems engineering and a master's degree in information security. He also holds a significant number of certifications, including CISSP, CISA, CISM, CRISC, ABCP and AWS Certified Security—Specialty, AWS Networking Specialty, and AWS Certified Solutions Architect.

Omner Barajas is a security specialist solution architect at Amazon Web Services in Latin America with more than 15 years of experience in cybersecurity. During those years, Omner has taken multiple roles as security consultant, IT architect, and security auditor while helping organizations from different industries to improve their security posture. Omner has a master's degree in information security and holds a significant number of certifications, including CISSP, CISA, CISM, AWS Certified Security—Specialty, AWS Certified Solutions Architect—Professional, and PCI Internal Security Assessor (ISA).

Rogerio Kasa is a Security Solutions Architect at Amazon Web Services (AWS), where he helps organizations strengthen their cloud security posture through strategic advisory and technical leadership. Since joining AWS in 2019, he has established himself as a trusted advisor in cloud security, leading the internal extended Security Community in Brazil, implementing risk-based security controls, governance frameworks, and compliance requirements. A certified professional holding CISSP/ISC2, CISM/ISACA, CCSK/CSA, and multiple AWS certifications, Rogerio combines deep technical expertise with strategic insight to help organizations navigate their cloud security challenges. His work spans security automation, incident response, network security, IAM, detection/response, data protection, and the implementation of comprehensive security controls across multi-account environments.

Contents at a Glance

Contents

Table of Exercises

Introduction

As the pioneer and world leader of cloud computing, Amazon Web Services (AWS) has positioned security as its highest priority. Throughout its history, the cloud provider has constantly added security-specific services to its offerings as well as security features to its ever-growing portfolio. Consequently, the AWS Certified Security—Specialty certification offers a great way for IT professionals to achieve industry recognition as cloud security experts and learn how to secure AWS environments, both in concept and practice.

According to the AWS Certified Security Specialty Exam Guide, the corresponding certification attests your ability to demonstrate the following:

- An understanding of specialized data classifications and AWS data protection mechanisms
- An understanding of data-encryption methods and AWS mechanisms to implement them
- An understanding of secure Internet protocols and AWS mechanisms to implement them
- A working knowledge of AWS security services and features of services to provide a secure production environment
- Competency from two or more years of production deployment experience in using AWS security services and features
- The ability to make trade-off decisions regarding cost, security, and deployment complexity to meet a set of application requirements
- An understanding of security operations and risks

Through multiple choice and multiple response questions, you will be tested on your ability to design, operate, and troubleshoot secure AWS architectures composed of compute, storage, networking, and monitoring services. It is expected that you know how to deal with different business objectives (such as cost optimization, agility, and regulations) to determine the best solution for a described scenario.

The AWS Certified Security—Specialty exam is intended for individuals who perform a security role for three to five years with at least two years of hands-on experience securing AWS workloads.

What Does This Book Cover?

To help you prepare for the AWS Certified Security Specialty (SCS-C02) certification exam, *AWS Certified Security Study Guide Specialty (SCS-C02) Exam, Second Edition* explores the following topics:

Chapter 1: Security Fundamentals This chapter introduces you to basic security definitions and foundational networking concepts. It also explores major types of attacks,

along with the AAA architecture, security frameworks, practical models, and other solutions. In addition, it discusses the TCP/IP protocol stack.

Chapter 2: Cloud Security Principles and Frameworks This chapter discusses critical AWS Cloud security concepts such as its shared responsibility model, AWS hypervisors, AWS security certifications, the AWS Well-Architected Framework, and the AWS Marketplace. It also addresses both security *of* the cloud and security *in* the cloud. These concepts are foundational for working with AWS.

Chapter 3: Management and Security Governance This chapter discusses strategies to govern your workloads effectively using multiple AWS accounts and AWS Organizations to centrally manage security services with delegated administration and applying guardrails such as SCPs (Service Control Policies) as a technical solution to enforce policies across your organization. It also addresses how AWS Control Tower helps to consistently deploy architectures based on best practices and security guardrails to protect your workloads.

Chapter 4: Identity and Access Management This chapter explores AWS Identity and Access Management (IAM), which establishes the foundation for all resource interactions within AWS accounts. It covers authentication methods through various interfaces (AWS Console, CLI, and SDKs) and explains how to implement authorization through policies and permissions. The chapter also addresses critical security features, including multifactor authentication, identity federation, and AWS Secrets Manager, while emphasizing best practices for securing AWS environments. Key concepts include role-based access, cross-account permissions, and the principle of least privilege.

Chapter 5: Security Logging and Monitoring This chapter discusses how to gather information about the status of your resources and the events they produce through a four-stage framework: resources state, events collection, events analysis, and action. Key services include AWS Config, CloudTrail, CloudWatch, Inspector, Security Lake, Systems Manager, Trusted Advisor, and EventBridge, which work together to provide comprehensive visibility and automated responses to security events in AWS environments.

Chapter 6: Infrastructure Protection This chapter explores AWS networking concepts such as Amazon VPC, subnets, route tables, and other features that are related to network address translation (NAT gateways and NAT instances) and traffic filtering (security groups and network access control lists). It also addresses AWS Elastic Load Balancing and how security services such as AWS Web Application Firewall can provide secure access to your cloud-based applications. Finally, it discusses the AWS Shield and AWS's unique approach to mitigate distributed denial-of-service attacks.

Chapter 7: Data Protection This chapter discusses protecting data using a variety of security services and best practices, including AWS Key Management Service (KMS), the cloud hardware security module (CloudHSM), and AWS Certificate Manager. It also covers creating a customer master key (CMK) in AWS KMS, protecting Amazon S3 buckets, and how Amazon Macie can deploy machine learning to identify personal identifiable information (PII).

Chapter 8: Threat Detection and Incident Response This chapter covers AWS threat detection services (including GuardDuty, Security Hub, Trusted Advisor, and Detective) and incident response procedures, emphasizing both manual and automated approaches to handling security incidents. It covers the incident response life cycle, common security scenarios, and best practices for creating and implementing response plans while leveraging AWS services and automation capabilities to detect and remediate security issues effectively.

Appendix A: Answers to Review Questions This appendix provides the answers to the review questions that appear at the end of each chapter throughout the book.

Appendix B: Creating Your Security Journey in AWS This appendix discusses how to create your strategy to improve your security posture, consistently prioritizing the most important initiatives that can provide you security benefits, such as mitigating critical risks as soon as possible, thus optimizing your team's results.

Appendix C: AWS Security Services Portfolio This appendix provides an overview of the 24 AWS cloud services dedicated to security, identity, and compliance.

Appendix D: DevSecOps in AWS This appendix introduces DevSecOps, the AWS family of services that implement DevOps practices, and how security controls can be implemented in an automated pipeline.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts, an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Interactive Online Learning Environment and Test Bank

Studying the material in the *AWS Certified Security Study Guide: Specialty (SCS-C02) Exam* is an important part of preparing for the AWS Certified Security Specialty (SCS-C02) certification exam, but we provide additional tools to help you prepare. The online test bank will help you understand the types of questions that will appear on the certification exam. The online test bank runs on multiple devices.

Sample Tests: The sample tests in the test bank include all the questions at the end of each chapter as well as the questions from the assessment test. In addition, there are two practice

exams with 50 questions each. You can use these tests to evaluate your understanding and identify areas that may require additional study.

Flashcards: The flashcards in the test bank will push the limits of what you should know for the certification exam. There are 100 questions provided in digital format. Each flashcard has one question and one correct answer.

Glossary: The online glossary is a searchable list of key terms introduced in this exam guide that you should know for the AWS Certified Security Specialty (SCS-C02) certification exam.

Go to `www.wiley.com/go/sybextestprep` to register and gain access to this interactive online learning environment and test bank with study tools. To start using these tools to study for the AWS Certified Security Specialty (SCS-C02) exam, go to `www.wiley.com/go/sybextestprep` to register your book and receive your unique PIN. Once you have the PIN, return to `www.wiley.com/go/sybextestprep`, find your book, and click register or login and follow the link to register a new account or add this book to an existing account.

AWS Certified Security Study Guide—Specialty (SCS-C02) Exam Objectives

This table shows the extent, by percentage, of each domain represented on the actual examination.

Domain	Percent of Examination
Domain 1: Threat Detection and Incident Response	14%
Domain 2: Security Logging and Monitoring	18%
Domain 3: Infrastructure Security	20%
Domain 4: Identity and Access Management	16%
Domain 5: Data Protection	18%
Domain 6: Management and Security Governance	14%
Total	100%

Exam objectives are subject to change at any time without prior notice and at AWS's sole discretion. Visit the AWS Certified Security–Specialty website (`aws.amazon.com/certification/certified-security-specialty`) for the most current listing of exam objectives.

Objective Map

Objective	Chapters
Domain 1: Threat Detection and Incident Response	
1.1: Design and implement an incident response plan.	2,8
1.2: Detect security threats and anomalies by using AWS services.	1,5,8
1.3: Respond to compromised resources and workloads.	8
Domain 2: Security Logging and Monitoring	
2.1: Design and implement monitoring and alerting to address security events.	1,5
2.2: Troubleshoot security monitoring and alerting.	5
2.3: Design and implement a logging solution.	5
2.4: Troubleshoot logging solutions.	5
2.5: Design a log analysis solution.	5
Domain 3: Infrastructure Security	
3.1: Design and implement security controls for edge services.	1,6
3.2: Design and implement network security controls.	1,6
3.3: Design and implement security controls for compute workloads.	6
3.4: Troubleshoot network security.	2,6
Domain 4: Identity and Access Management	
4.1: Design, implement, and troubleshoot authentication for AWS resources.	1,4
4.2: Design, implement, and troubleshoot authorization for AWS resources.	4
Domain 5: Data Protection	
5.1: Design and implement controls that provide confidentiality and integrity for data in transit.	7
5.2: Design and implement controls that provide confidentiality and integrity for data at rest.	7

Objective	Chapters
5.3: Design and implement controls to manage the life cycle of data at rest.	1,7
5.4: Design and implement controls to protect credentials, secrets, and cryptographic key materials.	7
Domain 6: Management and Security Governance	
6.1: Develop a strategy to centrally deploy and manage AWS accounts.	3
6.2: Implement a secure and consistent deployment strategy for cloud resources.	3
6.3: Evaluate the compliance of AWS resources.	3,5
6.4: Identify security gaps through architectural reviews and cost analysis.	3

Assessment Test

1. Which one of the following components should not influence an organization's security policy?
   - **A.** Business objectives
   - **B.** Regulatory requirements
   - **C.** Risk
   - **D.** Cost–benefit analysis
   - **E.** Current firewall limitations

2. Consider the following statements about the AAA architecture:

I. Authentication deals with the question "Who is the user?"

II. Authorization addresses the question "What is the user allowed to do?"

III. Accountability answers the question "What did the user do?"

Which of the following is correct?

- **A.** Only I is correct.
- **B.** Only II is correct.
- **C.** I, II, and III are correct.
- **D.** I and II are correct.
- **E.** II and III are correct.

3. What is the difference between denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks?
   - **A.** DDoS attacks have many targets, whereas DoS attacks have only one each.
   - **B.** DDoS attacks target multiple networks, whereas DoS attacks target a single network.
   - **C.** DDoS attacks have many sources, whereas DoS attacks have only one each.
   - **D.** DDoS attacks target multiple layers of the OSI model and DoS attacks only one.
   - **E.** DDoS attacks are synonymous with DoS attacks.

4. Which of the following options is incorrect?
   - **A.** A firewall is a security system aimed at isolating specific areas of the network and delimiting domains of trust.
   - **B.** Generally speaking, the web application firewall (WAF) is a specialized security element that acts as a full-reverse proxy, protecting applications that are accessed through HTTP.
   - **C.** Whereas intrusion prevention system (IPS) devices handle only copies of the packets and are mainly concerned with monitoring and alerting tasks, intrusion detection system (IDS) solutions are deployed inline in the traffic flow and have the inherent design goal of avoiding actual damage to systems.

D. Security information and event management (SIEM) solutions are designed to collect security-related logs as well as flow information generated by systems (at the host or the application level), networking devices, and dedicated defense elements such as firewalls, IPSs, IDSs, and antivirus software.

5. In the standard shared responsibility model, AWS is responsible for which of the following options?
   - **A.** Regions, availability zones, and data encryption
   - **B.** Hardware, firewall configuration, and hypervisor software
   - **C.** Hypervisor software, regions, and availability zones
   - **D.** Network traffic protection and identity and access management
6. Which AWS service allows you to generate compliance reports that enable you to evaluate the AWS security controls and posture?
   - **A.** AWS Artifact
   - **B.** AWS Trusted Advisor
   - **C.** AWS Well-Architected Tool
   - **D.** Amazon Inspector
7. Which of the following contains a definition that is not a pillar from the AWS Well-Architected Framework?
   - **A.** Security and operational excellence
   - **B.** Reliability and performance efficiency
   - **C.** Cost optimization and availability
   - **D.** Security and performance efficiency
8. Which of the following services provides a set of APIs that controls access to your resources on the AWS Cloud?
   - **A.** AWS AAA
   - **B.** AWS IAM
   - **C.** AWS Authenticator
   - **D.** AWS AD
9. Regarding AWS IAM principals, which option is *not* correct?
   - **A.** A principal is an IAM entity that has permission to interact with resources in the AWS Cloud.
   - **B.** They can only be permanent.
   - **C.** They can represent a human user, a resource, or an application.
   - **D.** They have three types: root users, IAM users, and roles.